TITLE:

# POLYADIC CODES(Algebraic Combinatorial Theory)

AUTHOR(S):

Pless, Vera

CITATION:

Pless, Vera. POLYADIC CODES(Algebraic Combinatorial Theory). 数理解析研究所講究録 1988, 671: 107-115

ISSUE DATE:

1988-09

URL:

http://hdl.handle.net/2433/100820

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

数理解析研究所講究録
第671巻 1988年 107-115

# POLYADIC CODES

Vera Pless

University of Illinois at Chicago
Chicago, Illinois 60680

Binary duadic codes were first defined in [2]. They generalize quadratic residue codes. Properties similar to properties of quadratic residue codes are demonstrated in a simple fashion for this more general class of codes and it turns out that more codes (than just quadratic residue codes) share these properties. Further, we were able to construct many of these codes easily. We found many new "good" codes. These were generalized to duadic codes over GF(q) in [3,6,7]. Triadic codes over GF(q) were defined in [4]. From these definitions it was not so easy to see how to generalize duadic and triadic codes to polyadic codes over GF(q). However this generalization is now given in [1]. In doing this we also defined m-adic residue codes. Before only quadratic residue and cubic residue codes were known. We now have a more general class of cubic residue codes and also m-adic residue codes for all m.

Duadic codes contain quadratic residue codes, Golay codes and many Reed-Muller and Reed-Solomon codes. These are "algebraically interesting" and "good" codes. All are cyclic codes so we will start with a brief introduction to cyclic codes. This is a very important family of codes so it is nice to know more about them. Our terminology is as in [5].

$\mathcal{C}$ is a cyclic code if $(c_0,c_1,\cdots,c_{n-1})$ is in $C$ implies $(c_{n-1},c_0,\cdots,c_{n-2})$ is also in $C$. Another way of saying this is that $\mathcal{C}$ is invariant under the coordinate permutation $i \to (i+1) \pmod n$.

If $F = GF(q)$, $F[x]$ is the set of all polynomials in $x$ with coefficients in $F$. We let g.c.d. $(q,n) = 1$. $R_n = F[x]/(x^n-1)$ is the set of all polynomials in $x$ of degree $<n$ with coefficients in $F$. It is known [5] that $R_n$ is a principal ideal ring (P.I.R.) with the usual polynomial addition and multiplication $\bmod(x^n-1)$. We suppose $n$ is odd.

We associate vectors in a cyclic code of length $n$ with polynomials in $R_n$ as in the following example.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | | |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | $\longleftrightarrow$ | $x + x^2 + x^4$ |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 | $\longleftrightarrow$ | $x^2 + x^3 + x^5$ . |

In this way a cyclic code is associated to an ideal in $R_n$. We can now multiply vectors. We identify a cyclic code with an ideal and a vector with a polynomial as above.

Since $R_n$ is a P.I.R. every vector in a cyclic code is a multiple of a generator polynomial (more than one). Two of these are distinguished. The generator polynomial is a factor of $x^n-1$. To find these polynomials one has to factor $x^n-1$ for each $n$ which is difficult when $n$ is large. The other distinguished generator is the idempotent generator $e(x)$. This satisfies $e(x)^2 = e(x)$ and $e(x)$ is the multiplicative unit of the ideal. For example, when $n = 7$ and $q = 2$, an idempotent generator of a code is $e(x) = x + x^2 + x^4$, $(x+x^2+x^4)^2 = x^2+x^4+x = e(x)$. The idempotent generators are easy to find in the binary case but not much is known about the code from them; the generator polynomial gives the dimension of its code. However idempotents have many nice algebraic properties and we will show how information about a code can be obtained from its idempotent under certain circumstances.

If $C$ has $e$ as idempotent generator, we denote this as $C = \langle e \rangle$.

Fact [5]: If $C_1 = \langle e_1 \rangle$ and $C_2 = \langle e_2 \rangle$, then $C_1 \cap C_2 = \langle e_1 e_2 \rangle$ and $C_1 + C_2 = \langle e_1 + e_2 - e_1 + e_2 \rangle$.

Let $\underline{h} = (1,\cdots,1)$ denote the all-one vector.

The following concepts arose in the study of duadic codes:

A vector $v = (a_0,\cdots,a_{n-1})$ is called even-like if $\sum_{i=0}^{n-1} a_i = 0$, otherwise it is called odd-like.

A code is called even-like if all its vectors are even-like, otherwise it is called odd-like.

Fact: A cyclic code C is odd-like iff h is in C.

Fact: If v is even-like, $vh = 0$. If v is odd-like, $vh = \alpha h$ where $\alpha \neq 0$.

Some examples of cyclic codes.

1) The whole space $V = \langle 1 \rangle$.

2) The $n-1$ dimensional space, E, of all even-like vectors. $E = \langle 1-\frac{1}{n} h \rangle$.

3) The one dimensional space, $\langle \frac{1}{n} h \rangle$.

Let g.c.d. (a,n) = 1. Then the coordinate permutation (which is like multiplication) $\mu_a: i \to ai \pmod n$ is important for our studies.

Fact [5]: If $C = \langle e \rangle$ is a cyclic code, then $\mu_a(C)$ is a cyclic code and $\mu_a(C) = \langle \mu_a(e) \rangle$.

Duadic codes are an infinite family of cyclic codes over GF(q) defined in terms of their generating idempotents.

Def: If $C_1 = \langle e_1 \rangle$ and $C_2 = \langle e_2 \rangle$ are even-like cyclic codes, then they are duadic codes if

1) There is a $\mu_a$ with $\mu_a(C_i) = C_j$ $i \neq j$, and

2) $e_1 + e_2 = 1-\frac{1}{n} h$.

Then $\langle 1-e_1 \rangle$ and $\langle 1-e_2 \rangle$ are odd-like duadic codes.

Many properties of these codes can be demonstrated. Among these are the following

1) dim $C_i = \frac{n-1}{2}$ .

2) $C_i$ exist iff q is a square (mod n).

3) Every self-orthogonal cyclic code of dim $\frac{n-1}{2}$ is duadic.

Property 3) is useful for studying some combinatorial designs with a cyclic group as they often generate a self-orthogonal cyclic code of dim $\frac{n-1}{2}$ . Then 2) gives one criterion for existence. There are others as the duadic codes must be interchanged by $\mu_{-1}$ in this situation.

We computed idempotents for binary duadic codes of prime lengths up to 241 and found many new, good codes.

Triadic codes are also an infinite family of cyclic codes over GF(q) defined in terms of their generating idempotents.

Def: The <u>even-like</u> codes $C_i = \langle e_i \rangle$, $i = 0,1,2$ are <u>triadic</u> if

1) There is a $\mu_a$ with $\mu_a(C_i) = C_{i+1}$ (mod 3) and

2) $e_0 + e_1 + e_2 - 2e_0e_1e_2 = 1 - \frac{1}{n} h$.

Then triadic codes exist iff q is a cubic residue (mod n) [4].

Polyadic codes generalize duadic codes. M-adic residue codes are polyadic codes which generalize quadratic residue codes. We will start with m-adic residue codes. These are new for $m > 2$. All codes are cyclic codes over GF(q).

It is known [5] that the whole space V is a direct sum of its minimal ideals one of which is $M_0 = \langle \frac{1}{n} h \rangle$ denoted by $\langle h' \rangle$. This decomposition is unique and leads to the following facts. If C and D are cyclic codes and $C \subseteq D$, then there is a unique cyclic code $C'$ so that $D = C + C'$ and $C \cap C' = 0$. We call $C'$ the <u>complement of</u> C <u>with respect to</u> D. If $D = V$, $C'$ is the <u>complement</u> of C.

For example, $V = M_0+(M_1+\cdots+M_r)$, where the $M_i$ are the minimal ideals not equal to $M_0$. Then $M_0=\langle h'\rangle$ and $(M_1+\cdots+M_r) = E$ are complements of each other.

If the length is a prime p, then all $M_i$ have the same dimension s and there is an r with

$$rs = (p-1).$$

It is easy to compute r and s from the cyclotomic cosets [5]. r is the number of non-zero cyclotomic cosets and s is their size. Further cyclotomic cosets are easy to compute. Here are some examples.

1) q=2, p=7: cyclotomic cosets: (1,2,4), (3,6,5) r=2, s=3

2) q=2, p=3

cyclotomic cosets: (1,2,4,8,16), (3,6,12,24,17), (5,10,20,9,18), (7,14,28,25,19), (11,22,13,26,21), (15,30,29,27,23)

r=6, s=5

3) q=3, p=13

Cyclotomic cosets: (1,3,9), (2,6,5), (4,12,10), (7,8,11)

r=4, s=3

As we will see, m-adic residue codes exist when m divides r. So quadratic residue codes exist for examples 1,2,3. Cubic residue codes exist for example 2. 4-adic residue codes exist for example 3 and 6-adic residue codes exist for example 2.

If $e = \sum_{i\in S} x^i$ is a binary idempotent, then S is a union of cyclotomic cosets. Idempotents of many m-adic residue codes can be easily computed in this situation. For example

$$\begin{matrix} 0\,1\,2\,3\,4\,5 \\ (0\,1\,0\,1\,0\,0) \end{matrix} \quad \text{and} \quad \begin{matrix} 0\,1\,2\,3\,4\,5\,6 \\ (0\,0\,0\,1\,0\,1\,1) \end{matrix}$$

are idempotents of odd-like quadratic residue codes in example 1.

It is not difficult to compute idempotents from cyclotomic cosets for codes over GF(4) and GF(8) and for other GF(q) information about the existence, number, and dimension of m-adic residue codes can be gotten from the cyclotomic cosets.

In order to define m-adic residue codes we need some further terminology. Let p be a prime. Let $\underline{G} = GF(p)^*$, the cyclic multiplicative group of non-zero elements in GF(p). Let $\underline{H}$ be the cyclic subgroup of G generated by q. Then $|H| = s$ and there is an a so that $\mu_a$ cyclically permutes the $M_i$.

Let $\underline{Q} = \{\alpha^m: \alpha \in G\}$. These are the m-adic residues.

M-adic residue codes are only defined of prime length p and only when q is an m-adic residue (mod p). It can be shown that q is an m-adic residue (mod p) iff m divides r.

We have 3 equivalent definitions of m-adic residue codes in terms of 1) ideals, 2) generating idempotents, and 3) generating polynomials [1].

We give the definitions in terms of ideals and generating idempotents here as these are the simplest.

Take an a so that Ha generates G/H. Let $C_i = \langle e_i \rangle$, $i=0,\cdots,n-1$ be a set of even-like cyclic codes. Then the $C_i$ are even-like m-adic residue codes of Class I if

| | ideal definition | | idempotent definition |
|---|---|---|---|
| 1) | $\mu_a(C_i) = C_{i+1}$ | 1') | $\mu_a(e_i) = e_{i+1}$ |
| 2) | $C_i \cap C_j = \{0\}$ | 2') | $e_i e_j = 0$ |
| 3) | $C_0 + \cdots + C_{n-1} = E$ | 3') | $e_0 + \cdots + e_{n-1} = 1-h'$ |

We can show that $\dim(C_i) = \frac{p-1}{m}$ [1].

The complements of the even-like m-adic residue codes of Class I are the odd-like m-adic residue codes of Class I, denoted by $\hat{C}_i = \langle e_i' \rangle$, $i = 0,\cdots,m-1 \cdot e_i' = 1-e_i$.

The following properties of these codes can be deduced from the properties of the even-like m-adic residue codes of Class I.

| | ideal properties | | idempotent properties |
|---|---|---|---|
| 1) | $\mu_a(\hat{C}_i) = \hat{C}_{i+1}$ | 1') | $\mu_a(e'_i) = e'_{i+1}$ |
| 2) | $\hat{C}_i + \hat{C}_j = V$ | 2') | $e'_i + e'_j - e'_i e'_j = 1$ |
| 3) | $\hat{C}_0 \cap \cdots \cap \hat{C}_{n-1} = M_0$ | 3') | $e'_0 \cdots e'_{n-1} = h'$ |

We can show that $\dim(\hat{C}_i) = p - \frac{(p-1)}{m}$.

The complement of the even-like m-adic residue codes of Class I with respect to E are the even-like m-adic residue codes of Class II.

We denote these by $D_i = \langle f_i \rangle$, $i=0,\ldots,m-1$. $f_i = 1-h'-e_i$. Their properties follow from those of the even-like codes of Class I.

| | ideal properties | | idempotent properties |
|---|---|---|---|
| 1) | $\mu_a(D_i) = D_{i+1}$ | 1') | $\mu_a(f_i) = f_{i+1}$ |
| 2) | $D_i + D_j = E$ | 2') | $f_i + f_j - f_i f_j = 1-h'$ |
| 3) | $D_0 \cap \cdots \cap D_{n-1} = \{0\}$ | 3') | $f_0 f_1 \cdots f_{n-1} = 0$ |

We can show that $\dim(D_i) = p-1-\frac{(p-1)}{m}$.

The complements of the even-like m-adic residue codes of Class II are the odd-like m-adic residue codes of Class II denoted by $\hat{D}_i = \langle f'_i \rangle$, $i = 0,\ldots,m-1$, $f'_i = 1-f_i = h'+e_i$. Their properties can be deduced as above

| | ideal properties | | idempotent properties |
|---|---|---|---|
| 1) | $\mu_a(\hat{D}_i) = \hat{D}_{i+1}$ | 1') | $\mu_a(f'_i) = f'_{i+1}$ |
| 2) | $\hat{D}_i \cap \hat{D}_j = M_0$ | 2') | $f'_i f'_j = h'$ |
| 3) | $\hat{D}_0 + \hat{D}_1 + \cdots + \hat{D}_{n-1} = V$ | 3') | $f'_0 + \cdots + f'_{n-1} = 1+(n-1)h'$ |

We can show that $\dim(\hat{D}_i) = 1+\frac{(p-1)}{m}$.

If $n = 2$ (quadratic residue codes), the 2 families coincide: $C_0 = D_1$, $C_1 = D_0$.

Over GF(2) we can compute the idempotents easily (given the cyclotomic cosets) for quadratic residue codes and cubic residue codes. We have partial knowledge for the other m-adic residue codes.

Vanessa Job has computed the minimum weights of all binary m-adic residue codes of length $\leq 127$. These are usually the largest possible weights as given in Verhoeff's recent table.

We will only define even-like polyadic codes of class I (the other 3 families can be defined in terms of these as for m-adic residue codes).

Let $C_i = \langle e_i \rangle$, $i = 0,\ldots,m-1$ be a set of even-like codes of length $n$. Let $a$ be such that g.c.d. $(a,n) = 1$. The $C_i$ are <u>polyadic of Class I</u> if

| | ideal definition | | idempotent definition |
|---|---|---|---|
| 1) | $\mu_a(C_i) = C_{i+1}$ | 1') | $\mu_a(e_i) = e_{i+1}$ |
| 2) | $C_i \cap C_j =$ F−a fixed cyclic code | 2') | the $e_i e_j$ are all equal |
| 3) | $C_0+C_1+\cdots+C_{m-1} = E$ | 3') | $e_0+e_1+\ldots+e_{m-1}-(m-1)e_0\cdots e_{m-1}=1-h'$ |

M-adic residue codes are (polyadic) m-adic codes of prime length with $F=\{0\}$ and <u>a</u> a generator of G/H. The next theorem is about general even-like m-adic codes of prime length.

Theorem [1]. Let $p$ be a prime and $s = \mathrm{ord}_p q$. Then $p-1=rs$. Let $m \geq 2$ be an integer. Then there exists a family $\{C_i\}$, $i=0,\ldots,m-1$ of even-like m-adic codes of length $p$ over GF(q) with $\dim C_i = k$ and $\dim(C_0 \cap C_1 \cap \ldots \cap C_{n-1}) = \ell$ iff

$$m|(p-1),$$

$$q \text{ is an m-adic residue (mod p) (iff } m|r)$$

$$k > \ell,\ s|k,\ s|\ell \text{ and } p-1 = mk-(n-1)\ell.$$

## REFERENCES


1. R. Brualdi, V. Pless, "Polyadic Codes", to appear in Applied Discrete Math.

2. J. S. Leon, J. M. Masley, V. Pless, "Duadic Codes", IEEE Trans. on Inform. Theory, IT-30 (1984), 709-714.

3. V. Pless, "Duadic Codes Revisited", Congressus Numerantium 59 (1987), pp. 225-233.

4. V. Pless, J. J. Rushanan, "Triadic Codes", Lin. Alg. Applics. 98 (1988), pp. 415-433.

5. V. Pless, "Introduction to the Theory of Error-Correcting Codes", John Wiley and Sons, New York 1982. Translated into Japanese by Noburu Ito.

6. J. J. Rushanan, "Generalized Q-Codes", Ph.D. Thesis, Caltech (1986).

7. M. H. M. Smid, "On Duadic Codes", Master's Thesis, Eindhoven University of Technology (1986).